Volume 3. Air Operator Technical Administration

CHAPTER 11. OPERATOR RECORDKEEPING

SECTION 2. ACCEPTANCE OR APPROVAL PROCESS

1791. GENERAL. This section contains information and guidance to be used by Principal Operations Inspectors (POI) when accepting or approving operator recordkeeping systems. The recordkeeping acceptance or approval process follows the general 5-step acceptance and approval process described in volume 1, chapter 4, section 6. The computer-based recordkeeping system is authorized in Operations Specification (OpSpec) A025.

1793. REGULATORY REQUIREMENTS. Section 121.683 requires that the Federal Aviation Administration (FAA) approve a part 121 operator's computer-based recordkeeping system. All other recordkeeping systems must be acceptable to the administrator (part 121 subpart V, Records and Reports). POIs shall determine that an operator's recordkeeping system is in compliance with applicable regulations.

1795. GUIDELINES FOR APPROVAL OR ACCEPTANCE. During initial certification, the operator should ensure that the initial compliance statement clearly describes the procedures to be used by the operator for the generation and maintenance of required records. The computer-based recordkeeping system is authorized in OpSpec A025. After certification, POIs shall conduct surveillance of an operator's records on a routine basis to ensure that the records are being maintained. POIs shall also ensure that the records continue to contain the required information to show compliance with Title 14 of the Code of Federal Regulations (14 CFR). The operator shall develop a section in its general operations manual (GOM) that provides detailed instruction on the use of the recordkeeping system. This GOM section must be provided to the POI as part of the GOM.

1797. LEGAL REQUIREMENTS OF ELECTRONIC SIGNING. The FAA requires that an electronic signing process meet the following criteria to be considered legally binding:

A. The signature must be unique to the person using it. Electronic signatures that incorporate digital signature technology meet this requirement by virtue of public/private key cryptography. The private key generated for the user and used for signing data is virtually unique.

B. The signature must be verifiable as belonging to the user. Digital signatures meet this requirement by referencing a person's digital certificate to authenticate the signatory's identity.

C. The signature must be under the sole control of the person using it. A digital signature is controlled by the very process used to access the private key that signs the data electronically. As the key is stored in a protected file encrypted with a personal password, the signatory is required to enter his/her password each and every time a signature is to be applied. As a result, the digital signature remains under the sole control of the person with the file containing the key and the password that unlocks it. This process is the electronic equivalent of applying a handwritten signature to a paper document.

D. The signature must be permanently attached to the data in a way that authenticates both the attachment of the signature to that data and the integrity of the data transmitted. Digital signatures achieve this by permanently embedding signatures into the document and invalidating them if any changes to the document's contents are detected. Using a hashing algorithm, the digital signature authenticates and permanently links the act of consent embodied by the signature to the exact contents of the signed document. Each time the document is opened, you can authenticate the signature and verify and detect whether data has been changed since the document was first signed. If a change is detected, the previously-applied digital signature in invalidated. The electronic version of a document with digital or electronic signature attached is used for the authentication. Therefore, the document file must be retained or archived for authentication purposes.

E. The signer must intend the signature to have the

same force and effect as a signature affixed by hand. Electronic signatures may also meet this standard if the following three items are covered. First, a person must use a unique user identification and private password within the applicable closed system each time he/she plans to electronically sign a document within that system. Second, they place a mark or a signature in the document that visually indicates the signer's intent. Last, they include the option of incorporating an affirmation message along with the mark or signature. All steps ensure that intent is clearly understood.

F. Electronic records submitted or maintained in accordance with procedures developed under this guidance, digital or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form.

1799. DIGITAL SIGNATURES, CERTIFICATES, PUBLIC KEY INFRASTRUCTURE (PKI) AND CERTIFICATE AUTHORITIES.

A. Digital Signatures. Digital signature technology is the foundation of a variety of security, e-business, and e-commerce products. Based on public/private key cryptography, digital signature technology is used in secure messaging, PKI, virtual private networks (VPN), web standards for secure transactions, and electronic signatures.

(1) Public/private key cryptography encrypts and decrypts data through the unique pairing of public and private keys. Private keys are kept secret and stored in a protected environment, such as on a smart card or in a password-protected file on a PC, whereas public keys are housed in publicly-accessible directories for use in decrypting messages. Digital signatures verify the origin of digitally-signed data using a public key to confirm that the data was encrypted with a private key. When combined with a hashing algorithm, digital signatures can also verify the integrity of data.

(2) Contrary to what its name may suggest, however, digital signature technology does not enable individuals to sign electronic data with the same effect as a handwritten signature. For this to occur, digital signature technology must be incorporated into a process that reproduces the basic elements of a handwritten signature. Such elements include that the signature be unique, verifiable, and under the sole control of the signatory. The process must also be able to authenticate signed data and effectively capture a signer's intention to authenticate, agree to, or be bound by the data that was signed.

(3) While the public and private key pairs used in a digital signature are unique and can authenticate data for a very simple process, signing applications are not simple processes. Without a process or an application, digital signatures on their own cannot electronically reproduce the key elements required of a binding handwritten signature.

(4) *Digital Certificates, PKI, and Certificate Authorities (CA).* When digital signature technology is used to authenticate a particular individual, that individual's public key is digitally signed with another private key to secure his/her identity. This process produces what is know as a digital certificate, which can be issued and managed in one of two ways: It can be self-issued or issued through a PKI.

(a) Self-Issued Certificate (not acceptable to the FAA). Also known as a self-signed certificate, it is produced when an individual signs his/her own certificate. The equivalent of a handwritten signature on paper, a self-signed certificate means the bearer alone can vouch for the authenticity of his/her identity. In these cases, verification of that identity occurs directly between the individual in question and the other parties involved in the transaction. Once approved, subsequent use of the individual's digital certificate can be trusted.

(b) Digital Certificates Using PKI (acceptable to the FAA). While self-issued certificates are the easiest to implement and manage, digital certificates can also be issued and managed using a PKI consisting of servers, databases, cryptographic applications, and policies. The PKI ensures that digital certificates are used under the sole control of an issuing organization, and can be revoked or suspended at a later date if an individual's status changes. Digital certificates using PKI can be issued and managed by a central person or department within an organization, or by a trusted third party (which is acceptable to the FAA) known as a Certificate Authority (CA) who assumes the liability of vouching for an individual's identity.

1801. - 1806. RESERVED.

[PAGES 3-959 THROUGH 3-960 RESERVED]